UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,183	12/08/2003	Herbert A. Little	555255012471	2882

89441 7590 11/13/2009

Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
ZEE, EDWARD	
ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
11/13/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

dlpejeau@jonesday.com
portfolioprosecution@rim.com

Office Action Summary	Application No.	Applicant(s)	
	10/730,183	LITTLE ET AL.	
	Examiner	Art Unit	
	EDWARD ZEE	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-19 and 24-33* is/are rejected.

7)☒ Claim(s) *3 and 20-23* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendments filed on 07/29/09. Claims 1, 3, 5, 10, 17, 19, 20 and 29-32 have been amended, Claim 33 has been added; Claims 1-33 are pending and have been considered below.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/27/09 has been entered.

Election/Restrictions

3. The restriction requirement between Species I and II, as set forth in the Office action mailed on 10/29/08, has been reconsidered in view of the new amendments to the claims of the elected invention. **The restriction requirement is hereby withdrawn.** Claims 11-16, directed to Species II are no longer withdrawn from consideration.

In view of the above noted withdrawal of the restriction requirement, applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

Once a restriction requirement is withdrawn, the provisions of 35 U.S.C. 121 are no longer applicable. See *In re Ziegler*, 443 F.2d 1211, 1215, 170 USPQ 129, 131-32 (CCPA 1971). See also MPEP § 804.01.

Claim Objections

4. **Claim 7** is objected to because of the following informalities: the Examiner notes that the instant claim introduces a *"particular user"* and appears to later refer to such a user as *"the user"*, which may be unclear in light of the plurality of users already introduced in the parent claim. The Applicant is kindly requested to amend the claim to "the particular user" or the like, in an effort to maintain consistency and clarity. Appropriate correction is required.

5. **Claim 31** is objected to because of the following informalities: the Examiner notes that line 8 of the instant claim recites *"...wherein the authentication information that is* ***stored in a data store*** *by the remote authentication system..."* appears to be in reference to the *"authentication information store"* recited in line 3 of the claim. The Applicant is kindly requested to amend the claim to "...wherein the authentication information that is stored in the authentication information store by the remote authentication system..." or the like, in an effort to maintain consistency and clarity. Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1, 2, 6-8, 10-12, 16, 18, 19 and 28-33 are rejected under 35 U.S.C. 102(b) as being anticipated by Dare et al. (5,684,950).

Claim 1: Dare et al. discloses a system for distributing authentication information to users of remote devices comprising:

a. an authentication information store on a computer-readable memory configured to store authentication information for a plurality of users*(database)* [column 5, lines 35-40];

b. a data processor executable authentication system configured to receive a request for authentication information for one of the plurality of users from a remote device*(authentication broker)* [column 5, lines 1-5];

c. wherein the request comprises identity information for use in determining whether the request is from one of the plurality of users*(user ID)* [column 5, lines 1-5];

d. wherein the authentication system retrieves from the authentication information store, based on the identity information, the authentication information for the one of the plurality of users*(a table look up is performed)* [column 5, lines 35-40];

e. wherein the authentication information for the one of the plurality of users is present in the authentication store prior to the receipt of the request for authentication information*(containing all the passwords)* [column 5, lines 35-40];

f. wherein the retrieved authentication information is provided to the remote device for use in authenticating a user that is requesting remote access to a computer network*(workstation can access a server using password)* [column 5, lines 40-45].

Claim 2: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication information is used in a two-factor authentication system [figure 3a].

Claim 6: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the identity information comprises user information and account information [column 5, lines 1-5].

Claim 7: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 6 above and further discloses that the identity information identifies a particular user and corresponding authentication information being requested, and is used by the authentication system to authenticate the user requesting the authentication information [column 5, lines 1-5].

Claim 8: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication information in the request is used by the remote device for two-factor authentication [figure 3a].

Claim 10: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication system does not provide the authentication information to the remote device because a match was not found in the authentication information store based upon the identity information [column 5, lines 5-10].

Claim 11: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication information comprises a password required for remote access to resources in the computer network, wherein

the password is not known to a user of the remote device but is required for access to the resources in the computer network [column 4, lines 60-65].

Claim 12: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses an access code required for remote access to resources in the computer network, wherein the access code is not known to a user of the remote device but is required for access to the resources in the computer network [column 4, lines 60-65].

Claim 16: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above, wherein the retrieved authentication information comprises a non-expiring password and is stored in a protected data store on the remote device [column 5, lines 35-40].

Claim 18: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the retrieved authentication information is used by the remote device to gain access to a corporate local area network(LAN) [column 3, lines 10-15].

Claim 19: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 18 above and further discloses that two-factor authentication is used in the LAN to authenticate a user requesting remote access to the LAN, wherein the retrieved authentication information is used in performing two-factor authentication in order to gain access to the LAN [figure 3a].

Claim 28: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the remote device is a desktop computer [column 3, lines 10-15].

Claim 29: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the remote device communicates with the authentication system over a communication system, wherein the communication system comprise a wide area network (WAN) and a wireless network gateway [column 3, lines 30-45].

Claim 30: Dare et al. discloses a method for distributing authentication information for remotely accessing computer resources, comprising:

a. receiving a request for the authentication information from a remote device, the request comprising identity information of a user of the remote device [column 5, lines 1-5];

b. wherein the authentication information is stored in an authentication data store [column 5, lines 35-40];

c. authenticating the user based on the identity information in the request [column 5, lines 1-5];

d. returning the authentication information to the remote device to authenticate a user requesting remote access to a computer resources based upon the returned authentication information [column 5, lines 35-40];

e. wherein the authentication information is present in the authentication data store prior to receiving the request for the authentication information [column 5, lines 35-40].

Claim 31: Dare et al. discloses an apparatus for handling authentication information for users of remote devices, comprising:

a. an authentication information store on a computer-readable memory configured to store authentication information for a user of a remote device, the authentication information provided by a remote authentication system [column 5, lines 35-40];

b. wherein a request for the authentication information from the remote device to the remote authentication system contains identity information [column 5, lines 1-5];

c. wherein the authentication information that is stored in a data store by the remote authentication system is provided to the remote device after the request is processed based upon the identity information contained in the request [column 5, lines 1-5];

d. wherein the authentication information is present in the authentication information store prior to receipt of the request [column 5, lines 35-40];

e. a data processor executable code generation system configured to retrieve the authentication information stored in the authentication information store [column 5, lines 35-40];

f. wherein access information is generated based upon the retrieved authentication information and is used to authenticate a user requesting remote access to a remote computer network [column 5, lines 40-45].

Claim 32: Dare et al. discloses a method for obtaining authentication information for remotely accessing a computer network, comprising:

a. providing a request from a user of a remote device to an authentication system for the authentication information that is stored in a data store by the authentication system [column 5, lines 35-40];

b. wherein the request comprises identity information for use by the authentication system to authenticate the user based on the identity information provided in the request [column 5, lines 1-5];

c. receiving by the remote device the authentication information from the authentication system [column 5, lines 35-40];

d. wherein the received authentication information is used to authenticate a user requesting remote access to the computer network [column 5, lines 40-45];

e. wherein the authentication information is present on the data store prior to the providing a request from a user [column 5, lines 35-40].

Claim 33: Dare et al. discloses a system as in Claim 1, wherein the authentication information store is on a non-volatile memory [column 5, lines 35-40].

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 4, 13-15, 17 and 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dare et al. (5,684,950) in view of Kefford et al. (6,880,079).

Claim 4: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1, but does not explicitly disclose that the request comprises an HTTP connection request.

However, Kefford et al. discloses a similar invention and further discloses that a request comprises an HTTP connection request [column 5, lines 60-67].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the disclosure of Dare et al. with the additional features of Kefford et al., in order to utilizing a common communication system, as suggested by Kefford et al. [column 5, lines 50-55].

Claims 13-15: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above, but does not explicitly disclose that the retrieved authentication information comprises an expiring password and/or access code which is valid for a short period of time, wherein the period of time is on the order of minutes.

However, Kefford et al. discloses a similar invention and further discloses that retrieved authentication information comprises an expiring password and/or access code which is valid for a short period of time, wherein the period of time is on the order of minutes [column 9, lines 25-40].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the disclosure of Dare et al. with the additional features of Kefford et al., in order to provide for secure transmission of information, as suggested by Kefford et al. [column 3, lines 5-20].

Claim 17: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above, but does not explicitly disclose that the retrieved authentication information comprises a seed from which access codes are to be generated by the remote device, wherein the seed is stored in a protected data store on the remote device.

However, Kefford et al. discloses a similar invention and further discloses that retrieved authentication information comprises a seed from which access codes are to be generated by the remote device, wherein the seed is stored in a protected data store on the remote device*(client decrypts the OTP)* [column 10, lines 15-25].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the disclosure of Dare et al. with the additional features of Kefford et al., in order to provide for secure transmission of information, as suggested by Kefford et al. [column 3, lines 5-20].

Claim 24: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above, but does not explicitly disclose that the remote device is a wireless mobile communication device.

However, Kefford et al. discloses a similar invention and further discloses the remote device is a wireless mobile communication device [column 3, lines 5-20].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the disclosure of Dare et al. with the additional features of Kefford et al., in order to provide for secure transmission of information, as suggested by Kefford et al. [column 3, lines 5-20].

Claim 25: Dare et al. and Kefford et al. disclose a system for distributing authentication information to users of remote devices as in claim 24 above, and Dare et al. further discloses that the remote device stores the authentication information in a data store [column 5, lines 35-40].

Claims 26 and 27: Dare et al. and Kefford et al. disclose a system for distributing authentication information to users of remote devices as in claim 25 above, but Dare et al. does not explicitly disclose the data store is implemented in a smart card or USB token.

However, Kefford et al. further discloses that the data store is implemented in a smart card or USB token [column 11, lines 40-55].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the disclosure of Dare et al. with the additional features of Kefford et al. in order to implement the invention using a common type of computer system, as suggested by Kefford et al. [column 11, lines 30-40]

10. Claims 5 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dare et al. (5,684,950) in view of Owen et al. (2004/0187018).

Claim 5: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above, but does not explicitly disclose that the request comprises a network password and a digital signature, wherein the network password and digital signature are verified by the authentication system before the authentication information is provided to the remote device.

However, Owen et al. discloses a similar invention and further discloses the request comprises a network password and a digital signature, wherein the network password and digital signature are verified by the authentication system before the authentication information is provided to the remote device*(function preferably includes the hashing of the challenge, PIN and first key of a asymmetric pair)* [page 3, paragraph 0025].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the disclosure of Dare et al. with the additional features of Owen et al., in order to effectively authenticate a user, as suggested by Owen et al. [page 7, paragraph 0071].

Claim 9: Dare et al. discloses a system for distributing authentication information to users of remote devices as in claim 8 above, but does not explicitly disclose that the identity information comprises a network password entered by the user of the remote device and a digital signature generated based on a transformation of at least a portion of the information in the request, a signature key and a signature algorithm.

However, Owen et al. discloses a similar invention and further discloses the identity information comprises a network password entered by the user of the remote device and a digital signature generated based on a transformation of at least a portion of the information in the request, a signature key and a signature algorithm*(function preferably includes the hashing of the challenge, PIN and first key of a asymmetric pair)* [page 3, paragraph 0025].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to further modify the disclosure of Dare et al. with the additional features of Owen et al., in order to effectively authenticate a user, as suggested by Owen et al. [page 7, paragraph 0071].

Allowable Subject Matter

11. **Claims 3 and 20-23** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDWARD ZEE whose telephone number is (571)270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Edward Zee/
Examiner, Art Unit 2435
November 8, 2009